Coordinating Agency:

Department of Homeland Security

Cooperating Agencies:

Department of Agriculture
Department of Commerce
Department of Defense
Department of Education
Department of Energy
Department of Health and Human Services
Department of the Interior
Department of Justice
Department of Labor
Department of State
Department of Transportation
Department of the Treasury
Department of Veterans Affairs
Environmental Protection Agency
Federal Energy Regulatory Commission
Intelligence Community
Nuclear Regulatory Commission
Office of Science and Technology Policy
U.S. Postal Service
Information Sharing and Analysis Center Council
Partnership for Critical Infrastructure Security

INTRODUCTION

Purpose

This annex describes policies, roles and responsibilities, and the concept of operations for assessing, prioritizing, protecting, and restoring critical infrastructure and key resources (CI/KR) of the United States and its territories and possessions during actual or potential domestic incidents. The annex details processes to ensure coordination and integration of CI/KR-related activities among a wide array of public and private incident managers and CI/KR security partners within immediate incident areas as well as at the regional and national levels. Specifically, this annex does the following:

- Describes roles and responsibilities for CI/KR preparedness, protection, response, recovery, restoration, and continuity of operations relative to National Response Framework (NRF) coordinating structures and National Incident Management System (NIMS) guiding principles.

- Establishes a concept of operations for incident-related CI/KR preparedness, protection, response, recovery, and restoration.[1]

- Outlines incident-related actions (including preresponse and postresponse) to expedite information sharing and analysis of actual or potential impacts to CI/KR and facilitate requests for assistance and information from public- and private-sector partners.

[1] Restoration is an element of recovery and, within the context of this annex, is defined as returning CI/KR services and site performance capabilities.

Scope

This annex addresses integration of the CI/KR protection[2] and restoration mission as a vital component of the Nation's unified approach to domestic incident management, which also may include CI/KR-related international considerations.

Critical infrastructure includes those assets, systems, networks, and functions—physical or virtual—so vital to the United States that their incapacitation or destruction would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters. Key resources are publicly or privately controlled resources essential to minimal operation of the economy and the government.[3]

CI/KR is organized into 17 sectors that together provide essential functions and services supporting various aspects of the American government, economy, and society. (See Table A-1 for a full list of sectors and designated Sector-Specific Agencies (SSAs).)

Processes outlined herein apply to Federal departments and agencies during incidents with potential or actual CI/KR impacts—and may apply to, or involve, incident managers and security partners[4] at other levels of government and the private sector, including CI/KR owners and operators.

CI/KR-related processes described in this annex utilize the unified risk-based approach for "steady-state" protection detailed in the National Infrastructure Protection Plan (NIPP). CI/KR requirements generated by the threat or incident at hand are coordinated through NRF and NIMS organizational structures. This applies to activities in the local incident area, as well as response and recovery activities outside the incident area, regionally, or nationally.

Policies

Policies for CI/KR protection and preparedness are established through the following authorities: Homeland Security Act of 2002; Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection; the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets; the National Strategy for Securing Cyberspace; and other relevant statutes, Executive orders, and Presidential directives.

HSPD-7 charges the Secretary of Homeland Security with responsibility for coordinating the overall national effort to enhance the protection of the CI/KR of the United States. The directive also designates SSAs with responsibility for coordinating planning-, preparedness-, and protection-related activities within each of the 17 CI/KR sectors. This approach provides the structure needed to address the unique characteristics and operating models of each of the sectors.

[2] National Infrastructure Protection Plan, 2006, Glossary, pg. 104, defines the term *protection* as "actions to mitigate the overall risk to CI/KR assets, systems, networks, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation. In the context of the NIPP, protection includes actions to deter the threat, mitigate vulnerabilities, or minimize consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities, such as hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, promoting work force surety, and implementing cyber security measures, among various others."

[3] National Infrastructure Protection Plan, 2006, Glossary of Key Terms, is the source for the definitions of critical infrastructure and key resources. These definitions are derived from the provisions of the Homeland Security Act of 2002 and HSPD-7.

[4] As defined in the NIPP, security partners include Federal, State, regional, tribal, local, or international government organizations; private-sector owners and operators and representative organizations; academic and professional entities; and not-for-profit and private volunteer organizations.

This annex does not alter or supersede existing:

- Statutory responsibilities for CI/KR protection, incident management, emergency management, or other related functions under the law.

- Regulatory, contractual, or other legal relationships between Federal agencies and the private sector.

- International agreements, treaties, or other agreements for incident management or between the U.S. Government and other countries.

The following sections provide an overview of the general authorities that guide CI/KR-related activities in the context of the NRF. This includes the NIPP, developed as the implementing structure for steady-state CI/KR protection; the Robert T. Stafford Disaster Relief and Emergency Assistance Act; and the Defense Production Act.

National Infrastructure Protection Plan

The NIPP and its associated CI/KR Sector-Specific Plans (SSPs) work in conjunction with the NRF and its supporting annexes to provide a foundation for CI/KR preparedness, protection, response, and recovery efforts in an all-hazards context.

In fact, day-to-day public-private coordination structures, information-sharing networks, and risk management frameworks used to implement NIPP steady-state CI/KR protection efforts continue to function and enable coordination and support for CI/KR protection and restoration for incident-management activities under the NRF.

The NIPP establishes the overall risk-based construct that defines the unified approach to protecting the Nation's CI/KR in an all-hazards context, and specifies procedures and activities to reduce risk to the Nation's CI/KR on a day-to-day basis, including:

- The risk management framework used to implement NIPP steady-state CI/KR protection efforts and provide the CI/KR protection and restoration dimension for incident management activities under the NRF.

- The sector partnership model that encourages the use of Sector Coordinating Councils (SCCs), Government Coordinating Councils (GCCs), and cross-sector coordinating councils to create an integrated national framework for CI/KR preparedness, protection, and restoration across sectors.

- The networked approached to CI/KR information sharing that provides for multidirectional CI/KR-related exchanges of actionable intelligence, alerts, warnings, and other information between and among various NIPP partners including: SSAs; State, tribal, and local entities; the Intelligence Community; law enforcement; Emergency Support Functions (ESFs); other Federal agencies and departments; and CI/KR owners, operators, and sector-based information-sharing mechanisms.[5]

[5] CI/KR sectors rely on information-sharing mechanisms such as Information Sharing and Analysis Centers (ISACs), which provide operational and tactical capabilities for information sharing and, in some cases, support for incident response activities. Originally recommended by Presidential Decision Directive 63 in 1998, ISACs are sector-specific entities that advance physical and cyber CI/KR protection efforts by establishing and maintaining frameworks for operational interaction between and among members and external security partners.

Complementing the NIPP, supporting SSPs provide the specific mechanisms required for full implementation of the NIPP risk management framework within each CI/KR sector and are developed by designated SSAs in close collaboration with sector security partners, ESFs, and other Federal agencies and departments.

The NIPP Value Proposition

The "value proposition" set forth in the NIPP articulates guiding principles for coordination and cooperation between the government at all levels and the private sector. In accordance with these principles, the Federal Government:

- Provides owners and operators timely, accurate, and actionable all-hazards information.
- Ensures owners and operators are engaged at senior executive and operational levels primarily through their respective SCCs and GCCs.
- Articulates benefits of a risk-based, cross-sector approach to preparedness, resilience, and protection.
- Works with owners and operators to clearly establish priorities for prevention, protection, and recovery.
- Provides specialized technical expertise for CI/KR-related preparedness, protection, and recovery.
- Coordinates with international allies and owners and operators on CI/KR priorities, risk assessments, mitigation, and restoration and recovery activities.

General Process for Requesting Federal Assistance

CI/KR-related protection, response, and recovery activities operate within a framework of mutual aid and assistance. Incident-related requirements can be addressed through direct actions by owners and operators or with government assistance provided by Federal, State,[6] tribal, or local authorities in certain specific circumstances.

Robert T. Stafford Disaster Relief and Emergency Assistance Act.[7] Disaster assistance programs generally offer support for incident-related repair, replacement, or emergency protective services needed for infrastructure owned and operated by government entities.

Stafford Act principles permit consideration of private-sector requests for assistance, but the application of these legal principles does not guarantee that needs or requests from private-sector entities will be met in all cases. A private-sector CI/KR owner or operator may receive direct or indirect assistance from Federal Government sources when the need:

[6] Consistent with the definition of "State" in the Homeland Security Act of 2002, all references to States within the CI/KR Support Annex are applicable to territories and include by reference any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States (Homeland Security Act of 2002).

[7] Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended by Public Law 106-390, October 30, 2000; § 5170b. ESSENTIAL ASSISTANCE {Sec. 403}

- Exceeds capabilities of the private sector and relevant State, tribal, and local governments;
- Relates to immediate threat to life and property;
- Is critical to disaster response or community safety; and
- Relates to essential Federal recovery measures.

The process for coordinating requests for assistance and information from private-sector CI/KR owners and operators is described in the Concept of Operations section of this annex.

The Defense Production Act (DPA) provides specific authority to expedite supply and strengthen production capabilities for CI/KR protection and restoration activities.[8] These authorities include use of the following:

- Priority ratings in the Defense Priorities and Allocations System on contracts and orders for industrial resources.[9]
- Financial incentives to expedite deliveries and expand supplies of materials and services.
- Agreements by the private sector to share information to coordinate management of critical supplies.
- Private-sector experts in government emergency preparedness, response, and recovery activities.

The Department of Homeland Security (DHS)/Federal Emergency Management Agency coordinates DPA authorities related to incident management before and during an incident, including: providing priority ratings on contracts and orders for industrial resources in cooperation with the Department of Commerce or relevant SSAs; developing guidance and procedures; coordinating DPA plans and programs; and providing technical assistance for all appropriate Federal agencies under the NRF and NIPP.

CONCEPT OF OPERATIONS

The concept of operations describes specific organizational approaches, processes, coordinating structures, and incident-related actions required for the protection and restoration of CI/KR assets, systems, networks, or functions within the impacted area and outside the impacted area at the local, regional, and national levels. The processes described herein are detailed further in standard operating procedures, field guides, and other related guidance developed collaboratively by DHS and the cooperating agencies to this annex.

The concept of operations uses the organizational structures and information-sharing mechanisms that are established in the NIPP for identifying, prioritizing, protecting, and restoring the Nation's CI/KR and describes protocols to integrate these steady-state organizational elements with NRF incident management organizational structures and activities.

[8] The Defense Production Act of 1950 (codified as amended by the Defense Production Act Reauthorization of 2003) is the primary authority to ensure the timely availability of resources for national defense and civil emergency preparedness and response. The DPA defines "national defense" to include critical infrastructure protection and restoration, as well as activities authorized by the emergency preparedness sections of the Stafford Act. Consequently, DPA authorities are available for activities and measures undertaken in preparation for, during, or following a natural disaster or accidental or man-caused event.

[9] The Defense Priorities and Allocations System regulation found in 15 CFR Part 700 implements the priorities and allocations authority of the DPA, ensures the timely availability of industrial resources for approved programs, and provides an operating system to support rapid industrial response to a national emergency.

Specifically, the concept of operations focuses on processes and actions for CI/KR-related:

- Situational awareness.
- Impact assessments and analysis.
- Information sharing.
- Requests for assistance or information from private-sector CI/KR owners and operators.

General

Addressing CI/KR-related prevention, protection, preparedness, response, and recovery requires cooperation and collaboration between and among CI/KR entities. A primary objective of this collaborative effort between the private-sector owners and operators; State, tribal, and local governments; nongovernmental organizations; and the Federal Government is to ensure that resources are applied where they offer the most benefit for mitigating risk, deterring threats, and minimizing the consequences of incidents.

DHS is responsible for leading, integrating, and coordinating the overall national effort to enhance CI/KR protection, including developing and implementing comprehensive, multitiered risk management programs and methodologies; developing cross-sector and cross-jurisdictional protection guidance and protocols; and recommending risk management and performance criteria and metrics within and across sectors. The DHS responsibilities for CI/KR support that are most applicable during incident response include:

- Identifying, prioritizing, and coordinating Federal action in support of the protection of nationally critical assets, systems, and networks, with a particular focus on CI/KR that could be exploited to cause catastrophic health effects or mass casualties comparable to those produced by a weapon of mass destruction.
- Establishing and maintaining a comprehensive, multitiered, dynamic information-sharing network designed to provide timely and actionable threat information, assessments, and warnings to public- and private-sector security partners. This responsibility includes protecting sensitive information voluntarily provided by the private sector and facilitating the development of sector-specific and cross-sector information-sharing and analysis systems, mechanisms, and processes.
- Coordinating, facilitating, and supporting comprehensive risk assessment programs for high-risk CI/KR, identifying protection priorities across sectors and jurisdictions, and integrating CI/KR protective programs with the all-hazards approach to domestic incident management described in HSPD-5.
- Identifying and implementing plans and processes for threat-based increases in protective measures that align to all-hazards warnings, specific threat vectors as appropriate, and each level of the Homeland Security Advisory System (HSAS).
- Conducting modeling and simulations to analyze sector, cross-sector, and regional dependencies and interdependencies, to include cyber-related issues, and sharing the results with security partners, as appropriate.
- Integrating national efforts for the protection and recovery of CI/KR, including analysis, warning, information sharing, vulnerability reduction, and mitigation activities and programs.

- Documenting and sharing lessons learned from exercises, actual incidents, and predisaster mitigation efforts and applying those lessons, where applicable, to CI/KR protection efforts.

- Working with the Department of State, SSAs, and other security partners to ensure that U.S. CI/KR protection efforts are fully coordinated with international partners.

Federal departments and agencies provide support consistent with their CI/KR-related statutory or regulatory responsibilities or with their designated functions as SSAs, ESF primary or supporting agencies, or coordinating or cooperating agencies for other related NRF Support or Incident Annexes.[10]

SSAs focus on overarching CI/KR protection, risk management, and information sharing by working collaboratively with SCCs, GCCs, relevant Federal departments and agencies, State and local governments, ESFs, CI/KR owners and operators, sector-based information-sharing mechanisms, and other private-sector entities.

SSAs coordinate CI/KR efforts within their sectors to deter threats, mitigate vulnerabilities, and minimize consequences of manmade and natural incidents. SSPs specify each sector's approach to the risk management and information-sharing components of incident management.

In cooperation with the DHS Office of Infrastructure Protection (DHS/OIP), SSAs collaborate with private-sector security partners to encourage:

- Supporting comprehensive risk assessment and management programs for high-risk CI/KR.

- Sharing real-time incident notification as well as CI/KR protection practices and processes.

- Developing information-sharing and analysis mechanisms to include consideration of physical and cyber threats.

- Promoting security-related information sharing among public and private entities.

In the context of incident management, SSAs coordinate with their counterparts designated within various NRF, ESF, Incident, or other Support Annex functions, as appropriate.

ESFs are activated to provide support for evolving CI/KR-related incident management requirements by:

- Providing authorities, resources, program implementation, and support required for infrastructure-related response, recovery, and restoration within the impacted area.

- Serving as key points of coordination to address CI/KR issues and concerns relating to the impacted area.

- Coordinating and collaborating with DHS; SSAs; owners and operators; State, tribal, and local entities; ESFs; and others as required to address CI/KR concerns that fall within the scope of their ESF or other NRF-related responsibilities.

[10] Further discussion of specific Federal department and agency support for the CI/KR support activities is in the Roles and Responsibilities section of this annex.

State, tribal, and local government entities establish security partnerships, facilitate information sharing, and enable planning and preparedness for CI/KR protection within their jurisdictions. State governments are responsible for:

- Developing and implementing statewide or regional CI/KR protection programs integrated into homeland security and incident management programs.

- Serving as crucial coordination hubs, bringing together prevention, preparedness, protection, response, and recovery authorities, capacities, and resources among local jurisdictions, across sectors, and across regional entities.

- Acting as conduits for requests for Federal assistance when the threat or incident situation exceeds the capabilities of public- and private-sector security partners in their jurisdictions.

Tribal governments are responsible for public health, welfare, safety, CI/KR protection, and continuity of essential services within their jurisdictions.

Local governments usually are responsible for emergency services and first-level responses to CI/KR incidents. In some sectors, local governments own and operate CI/KR such as water, wastewater, and storm water systems and electric utilities, and are responsible for initial prevention, response, recovery, and emergency services provision.

Private-sector CI/KR owners and operators are responsible at the corporate and individual facility levels for risk and incident management planning, security, and preparedness investments. Other activities that form part of business and continuity of operations planning activities include:

- Developing and revising business continuity and emergency management plans to address direct effects of incidents and critical dependencies and interdependencies at sector, enterprise, and facility levels.

- Building increased resiliency, backup capabilities, and redundancy into business processes and systems.

- Maintaining coordination with incident management, information-sharing, and CI/KR protection programs.

- Reporting CI/KR status using established mechanisms for inclusion in the national common operating picture (COP).

- Developing and coordinating CI/KR protective and emergency-response actions, plans, and programs.

- Guarding against insider threats.

- Providing technical expertise to DHS, SSAs, ESFs, and other Federal, State, tribal, and local entities.

- Identifying CI/KR and prioritizing related protection and restoration activities.

ORGANIZATION

National Level

National organizational structures described in the NRF and NIPP provide formal and informal mechanisms for public- and private-sector coordination, situational awareness, impact assessments, and information sharing in regard to CI/KR-related concerns on a sector-by-sector and/or a cross-sector basis.

This coordination allows for broader engagement in one or more affected sectors. It also allows sectors to plan for and quickly react to far-reaching effects from an incident (or multiple incidents) and to alert individual owners and operators of the need to take specific actions to minimize impacts.

CI/KR support at the national level involves active participation and coordination across a variety of activities to include the exchange of liaisons, implementation of reporting and information-sharing protocols, and/or physical representation, as required, at the following:

- **National Operations Center (NOC).** Representatives are assigned to various components of the NOC to provide CI/KR subject-matter expertise and facilitate coordination, risk assessment, protective measure implementation, and information sharing. These representatives work with SSAs and ESF counterparts to ensure that coordinated CI/KR-related communications, planning, and responses occur. (The NRF base document provides further discussion of NOC components and functions.)

- **National Response Coordination Center (NRCC).** DHS/OIP assigns a liaison to the NRCC to provide CI/KR protection and incident management subject-matter expertise and reach-back capabilities to the National Infrastructure Coordinating Center, DHS/OIP risk assessment entities, SSA and ESF primary and supporting agencies, and Infrastructure Liaisons deployed to support Joint Field Office (JFO) functions.

- **National Infrastructure Coordinating Center (NICC).** The NICC is a 24/7 watch coordination center providing integrated CI/KR-related situational awareness and national-level coordination for SCCs, SSAs, owners/operators, and relevant regulatory authorities. The NICC collects sector and cross-sector status information and produces consolidated CI/KR reports for incorporation into the Federal interagency COP that is produced by the NOC. During incident response, the NICC works closely with the NRCC to enable overall Federal CI/KR response coordination and emergency management program implementation.

- **Department of Justice/Federal Bureau of Investigation (DOJ/FBI) Strategic Information and Operations Center (SIOC).** DHS/OIP designates representatives, as required, to serve as liaisons to the DOJ/FBI SIOC, which is the focal point and operational control center for all Federal intelligence, law enforcement, and investigative law enforcement activities related to domestic terrorist incidents or credible threats, including leading attribution investigations. The CI/KR representatives provide situational awareness, assessment, information-sharing support, and reach-back relating to CI/KR status, risk, consequences, and national-level sector and cross-sector priorities.

- **National Coordinating Center for Telecommunications (NCC).** The NCC is a joint government-industry sector forum that provides a mechanism for jointly responding to National Security and Emergency Preparedness (NS/EP) and other communications incidents. The NCC is the operational component of the National Communications System (NCS) and the lead Federal office for communications incident management. (Further details on the NCC and NCS are included in the ESF #2 – Communications Annex.)

- **United States Computer Emergency Readiness Team (US-CERT).** US-CERT is a 24/7 single point of contact for cyberspace analysis, warning, information sharing, incident response, and recovery for security partners. The partnership between DHS and public and private sectors is designed to enable protection of cyber infrastructure and to coordinate the prevention of and response to cyber attacks across the Nation. (Further information on US-CERT incident-related activities is included in the Cyber Incident Annex.)

- **Other Federal Department and Agency Emergency Operations Centers.** DHS/OIP designates liaisons, as required, to various Federal emergency operations centers depending on the nature of the threat or incident.

The CI/KR support actions described in this annex are applicable to incident management activities required for natural disasters and the full spectrum of terrorist events. The CI/KR support activities are flexible and adaptable to align to the specific requirements of the incident and function in conjunction with processes as described in the NRF and the various Incident Annexes: Biological, Catastrophic, Cyber, Food and Agriculture, Mass Evacuation, Nuclear/Radiological, Oil and Hazardous Materials, and Terrorism Incident Law Enforcement and Investigation.

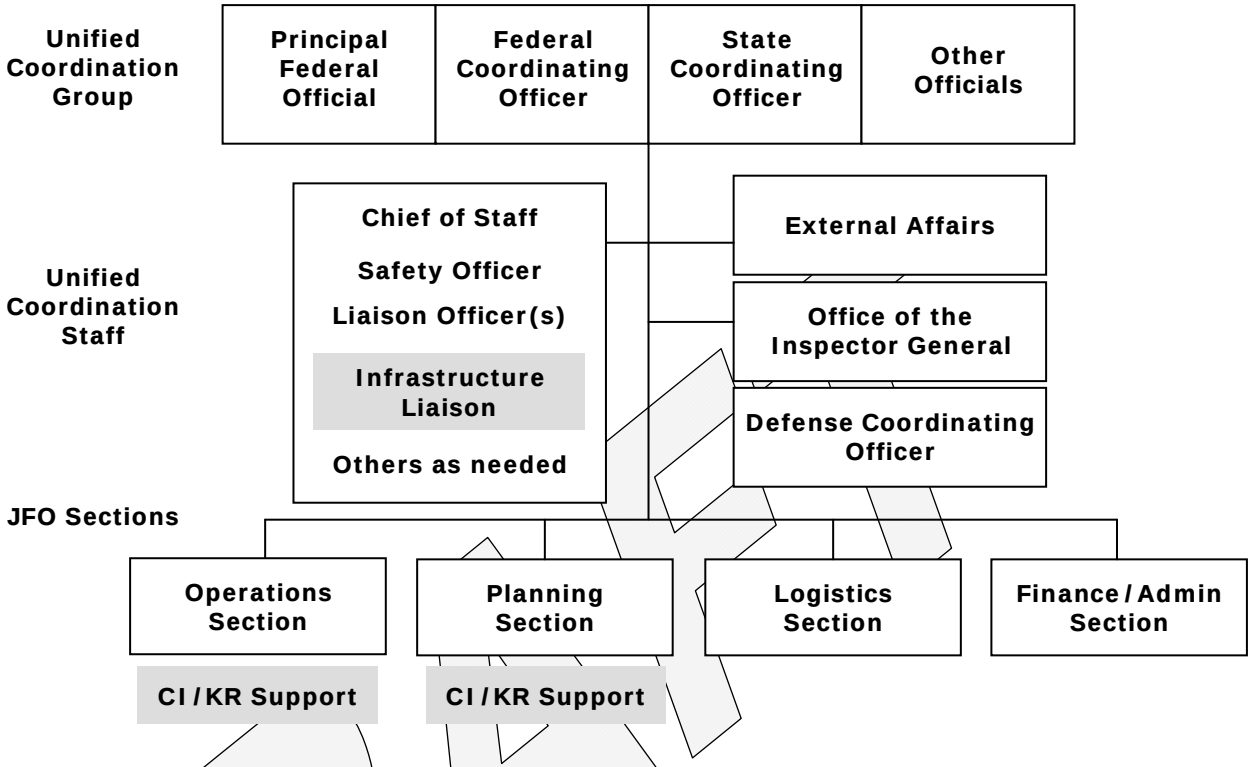
Field Level

The JFO, when established, provides the focal point for field-level incident-related CI/KR identification, assessment, prioritization, protection, and restoration activities.

CI/KR support is also provided, as required, to other incident facilities that are established to support prevention, preparedness, response, and recovery activities. These facilities include, but are not limited to: State, tribal, local, or county emergency operations centers; Incident Command Posts; Area and Unified Commands; and interim operating facilities.

The following section describes the integration of the Infrastructure Liaison functions to support the various JFO sections or field facilities, as well as day-to-day risk management expertise provided by DHS/OIP. (See Figure 1.)

Figure 1. JFO Organization



The Infrastructure Liaison is designated by DHS/OIP and advises the Principal Federal Official (PFO) (if appointed) and the Unified Coordination Group with regard to national- and regional-level and cross-sector CI/KR incident-related issues.

The Infrastructure Liaison function is task organized and task dependent on the needs of the incident and the requirements of the PFO, the Unified Coordination Group, and the Incident Management Team.

The Infrastructure Liaison, in collaboration with SSAs and all activated ESFs, provides prioritized recommendations regarding CI/KR concerns to the Unified Coordination Group and the PFO (if appointed). The prioritized CI/KR recommendations are developed using a collaborative process involving the cooperating agencies to this annex as well as CI/KR owners/operators; State, tribal, and local entities; and others as appropriate. The prioritized recommendations are used by the Unified Coordination Group to support incident-related decisionmaking processes and the efficient application of limited resources within the affected area.

The Infrastructure Liaison provides knowledge and expertise regarding unique CI/KR considerations, including:

- Impacts to nationally and regionally critical CI/KR within the incident area.
- Cross-sector impacts within the incident area.
- Cascading effects that can result in consequences beyond the immediate incident area.
- Interdependencies that require actions beyond those needed for infrastructure restoration within the incident area.

- Potential gaps or overlapping responsibilities among Federal departments and agencies that may function as SSAs, ESF primary or supporting agencies, or statutory or regulatory authorities.[11]

Infrastructure Liaison responsibilities include the following:

- Advising the Unified Coordination Group and the PFO, if appointed, on CI/KR issues with national or regional implications or that involve multiple CI/KR sectors.
- Acting as the coordination point for CI/KR sectors, including private-sector owners and operators, that are not otherwise represented in the JFO.
- Serving as the senior advocate in the Unified Coordination Staff for CI/KR issues not otherwise raised through the Unified Coordination Group.
- Advising the Unified Coordination Group regarding the prioritization of CI/KR protection and restoration issues.
- Providing additional coordination and liaison capabilities to the CI/KR sectors for the Unified Coordination Group in addition to the coordination and liaison functions provided by the various ESFs.
- Working with the JFO section and branch chiefs to coordinate between and among CI/KR sectors and ESFs.
- Ensuring that information obtained from the NICC and CI/KR sectors is integrated into the overall COP for the incident.

The Infrastructure Liaison assigns personnel as requested by the Unified Coordination Group to facilitate cross-sector and sector-related coordination and integration among ESFs, SSAs, appropriate Federal agencies and departments, and other entities with CI/KR-related responsibilities.

DHS/OIP provides training and designates Infrastructure Liaisons and other CI/KR support from a group that includes DHS/OIP Headquarters and/or field-level staff such as DHS/OIP Protective Security Advisors (PSAs)[12] and individuals with CI/KR expertise from other Federal departments and agencies, including SSAs and ESFs, as appropriate.

Infrastructure Liaison functions are task oriented depending on the scope, magnitude, and complexity of the CI/KR-related requirements. These functions include, but are not limited to:

- Assisting with on-site assessments of the status of potentially affected or impacted CI/KR.
- Deploying to other locations, such as State or local emergency operations centers (EOCs) or the JFO, to provide CI/KR subject-matter expertise.
- Providing assessments of local CI/KR status to the JFO based on direct observation and coordination with ESFs and CI/KR owners/operators.

[11] See Responsibilities section for discussion of SSA and ESF functions and a matrix of Federal department and agency functions.

[12] PSAs are DHS locally based critical infrastructure and vulnerability assessment specialists assigned to local communities throughout the country. PSAs serve as CI/KR liaisons between Federal agencies; State, tribal, and local governments; and the private sector. They contribute to NIPP- and NRP-related requirements by identifying, assessing, and monitoring CI/KR and coordinating protective activities within their respective geographic areas during steady-state operations as well as during incidents.

- Providing CI/KR-protection expertise in support of ESF #13 – Public Safety and Security efforts within an impacted area.

- Coordinating with SSAs, ESFs, and appropriate Federal agencies and departments on damage and security assessments to promote communication of assessment results and minimize duplication of effort.

CI/KR Support for Incident Management Actions

The CI/KR support function is structured to apply the NIPP risk management framework to produce prioritized recommendations for CI/KR protection and restoration in the context of incident management. DHS, cooperating agencies, and other government and private-sector security partners continuously conduct situational awareness, assessments, analyses, and information-sharing activities and facilitate requests for information and assistance through steady-state activities to better prepare for response, recovery, and restoration actions during an incident.

Key elements of these "steady-state" CI/KR support missions include:

Situational Awareness

- Monitoring information flow and threats to become aware of an incident or potential incident.

- Reviewing CI/KR data and data inventories.

- Identifying opportunities for mitigation.

- Identifying appropriate response posture for CI/KR elements and resources.

Assessments and Analyses

- Leveraging institutional knowledge and sector-partner relationships to collect data and assess CI/KR needs and vulnerabilities.

- Collaborating in preparation for more indepth assessments and analyses during an incident.

- Reviewing plans to assess projected impacts on CI/KR within a potential incident area.

- Developing projected consequences locally, regionally, and nationally by applying the NIPP risk management framework to the National Planning Scenarios.

The National Infrastructure Simulation and Analysis Center (NISAC) provides advanced modeling and simulation capabilities for the analysis of CI/KR vulnerabilities and interdependencies and the cascading effects of infrastructure loss, damage, or destruction over time based on the National Planning Scenarios.

Information Sharing

- Participating in multidirectional information flow between government and private-sector security partners.

- Developing and providing a comprehensive COP of threats and hazards to CI/KR.

- Providing security partners with a robust communications network, including a common set of communications, coordination, and information-sharing capabilities.

- Providing a means for State, tribal, local, and private-sector security partners to be integrated, as appropriate, into the intelligence cycle.

Requests for Information/Assistance

- Facilitating real-time transmission of requests and status.

- Maintaining a comprehensive log and retrievable database of all requests.

During daily operations (non-incident related), the NICC disseminates a range of all-hazards products and CI/KR protection information to security partners. Information dissemination includes the following:

- Threat-related and other all-hazards information products to government and private-sector CI/KR security partners, as appropriate.

- Reports from the private sector on suspicious activity or potential threats to the Nation's CI/KR.

- Requests for information and requests for assistance.

Preresponse/Initial Actions

Transition from steady-state to preresponse incident-related activities begins with warning of a potential incident or the notification of an incident.

CI/KR Information, Assessment, and Analytical Products

Examples of DHS information, assessment, and analytical products include:

- **Incident Reports:** Evaluate information received initially through news media, Internet, CI/KR owners and operators, and other sources.

- **Spot Reports:** Provide current situation status and operational snapshot assessment of operational CI/KR effects from emerging incidents.

- **Threat Warnings:** Fuse all source information to provide analysis of emergent threats on a timely basis.

- **Terrorist Target Selection Matrix:** Identifies sectors prone to different terrorist attack modalities.

- **Attack-Specific Threat Scenarios:** Provide planning and exercise phases for possible attacks with inputs from corporate- or facility-level security officers.

- **Sector-Specific Threat Assessment:** Provides specific and general terrorist threat information for each sector, as well as relevant background information, such as terrorist objectives and motives as they apply to that sector.

Notification and Reporting

DHS, in coordination with the SSAs, is responsible for coordinating CI/KR incident notification and information sharing among Federal agencies; State, tribal, and local entities; and CI/KR owners/operators. DHS uses established systems, such as the Homeland Security Information Network (HSIN), COP, Critical Infrastructure Warning Network, and other sector-based information-sharing mechanisms, to create CI/KR situational awareness in support of incident operations.

Upon notification from the NOC of a potential or actual incident, the NICC coordinates with the SSAs, CI/KR sectors (GCCs and SCCs), ESFs, industry partners, and other established information-sharing mechanisms to communicate pertinent information.

Based on the nature and scope of the potential or actual incident, DHS/OIP alerts and, if required, deploys Infrastructure Liaisons or additional CI/KR support to various NOC elements, the DOJ/FBI SIOC, or other Federal emergency operations centers or to field facilities to ensure full integration of CI/KR considerations and to provide situational awareness, assessments, information sharing, and prioritized recommendations.

In support of NOC reporting requirements, the NICC serves as the overall Federal focal point for CI/KR incident and status reporting from SSAs, ESFs, CI/KR owners/operators, and other appropriate Federal and/or State departments and agencies. The NICC coordinates these inputs with the NRCC and JFO. The following actions occur when reporting starts:

- The NICC alerts SSAs that the reporting process has begun via the Infrastructure Protection Executive Notification Service.

- SSAs coordinate with SCCs, GCCs, ESFs, and established information-sharing and analysis mechanisms in their sector to initiate status reporting and impact assessments. (These can include various sector-identified information-sharing mechanisms such as Information Sharing and Analysis Centers (ISACs) or Information Sharing and Analysis Organizations (ISAOs).

- The NICC verifies reported information and compiles the CI/KR Situation Report, which is included in the NOC COP and posted to the HSIN.

- Cooperating agencies are responsible for notifying DHS when they receive threat- or incident-related information from within their sectors. The NICC documents these reports, compiles additional details surrounding the suspicious activity or potential threat, and disseminates reports to the CI/KR sectors, the NOC, the NRCC, the DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), and DOJ/FBI.

CI/KR-related threat analysis is a collaborative function between the DHS Office of Intelligence and Analysis (DHS/OI&A) and OIP through the DHS HITRAC, which conducts integrated terrorism threat and risk analysis for all CI/KR sectors.

DHS/OI&A works with the intelligence and law enforcement communities to assess national security threats.[13] HITRAC brings together both intelligence and infrastructure specialists to provide an understanding of CI/KR sector- and national-level risk. This collaborative function is carried out with:

- Input from private-sector liaison personnel, and on-call subject-matter experts who provide industry-specific expertise.
- Input from the intelligence and law enforcement communities.
- Coordination with existing entities such as NCC, US-CERT, GCCs, SCCs, SSAs, ESFs, and/or other sector-identified information-sharing and analysis organizations such as ISACs.

On the basis of HITRAC analysis, DHS produces information that supports the response to emergent threats or immediate incidents, as well as strategic planning activities focused on enhancing the protection of CI/KR over the long term.

CI/KR risk assessment and analysis is a collaborative effort between DHS, cooperating agencies to this annex, and other security partners to perform the following:

- Examine existing plans and infrastructure characteristics to assess projected or actual impacts on CI/KR in potential incident areas or on CI/KR that have been designated as high risk.
- Determine critical failure points within or across CI/KR sectors, regional or national cascading effects, and other significant issues that could affect CI/KR assets inside and outside the immediate incident area.

The risk assessment and analysis process uses empirical data collection, database development and assessment, modeling, and simulation to inform decisionmaking.

These assessments and analyses support CI/KR protection and mitigation actions prior to an incident and timely response actions during an incident. Results of assessments and analyses are provided to the NICC, SSAs, ESFs, emergency managers, CI/KR owners and operators, and appropriate Federal and State departments and agencies.

The NIPP details protective programs and initiatives that provide the basis for CI/KR risk assessment activities during incident management. The following are representative of these key processes:[14]

- **National Asset Data Base (NADB):** Comprehensive catalog of the Nation's assets, systems, and networks and the primary Federal repository for CI/KR information.
- **Buffer Zone Protection Program:** Grant program to provide resources to State, tribal, and local law enforcement and other security professionals to enhance security of priority CI/KR facilities.
- **Site Assistance Visits:** Facility-level security assessments to facilitate vulnerability identification and mitigation discussions.

[13] See the Terrorism Incident Law Enforcement and Investigation Annex in the NRF for a complete discussion on threat investigation-related actions.

[14] See Appendix 3B in the NIPP for a complete listing and description of each.

The NISAC provides advanced modeling and simulation capabilities for the analysis of CI/KR vulnerabilities and interdependencies and the cascading effects of infrastructure loss, damage, or destruction over time.

During emerging or actual incidents, the NISAC produces assessments that:

- Integrate current situation data with preestablished infrastructure modeling, simulation, and analysis.
- Project consequences of an incident, preincident or postincident.
- Inform response and recovery activities after an incident has occurred.

Additional CI/KR support preresponse actions include:

- Testing and exercising information-sharing and communication processes and systems with CI/KR protection security partners.
- Developing and testing continuity of business plans, including identification and preparation of alternate sites and backup locations, as appropriate.
- Recommending and implementing elevated protective measures to align the CI/KR protective posture with all-hazards warnings, specific threat indications, and different levels of the HSAS.
- Preparing the Infrastructure Liaison and CI/KR support to deploy to the JFO.

RESPONSE ACTIONS

CI/KR situational awareness and reporting are essential to providing a consolidated COP during an incident. The NICC provides coordinated CI/KR status and infrastructure-related information supporting the COP by serving as the national collection, reporting, and distribution point for CI/KR-related information.

The NICC provides a focus on CI/KR-related impacts both within the incident area and across the Nation as a whole. It provides mechanisms to integrate and cross-reference CI/KR-related information from various official sources to minimize duplicative reporting and information collection.

In support of incident response, the NICC performs the following:

- Hosts a daily teleconference to provide owners and operators and SSAs, ESFs, and other Federal departments and agencies with a collated CI/KR status and facilitates cross-sector discussions
- Provides tailored situation assessments for the CI/KR section of the DHS Situation Report.
- Facilitates assessment sessions between SSAs and DHS Sector Specialists.
- Reconciles CI/KR information and reporting with the NRCC.
- Consolidates SSA reports for integration into overall national-level reporting, including the COP.

- Provides security partners with Web-enabled access to a variety of incident-related information.

SSAs, ESFs, and other Federal departments and agencies maintain situational awareness of their area of responsibility and factor information from official field-level sources into their overall sector-level reporting.

Established protocols for SSA CI/KR reporting include producing field-level reports (as applicable) and analyzing the national-, regional-, and sector-level CI/KR implications. All information is coordinated with appropriate entities. These products are created for, but not limited to, the following categories of information:

- Current status/damage assessments
- Restoration activities
- Key issues and concerns

CI/KR incident reporting cycles are synchronized with the overarching reporting requirements established by the NOC and NRCC at the national level and by the JFO or multiple JFOs, as required, at the field level.

Field-level reporting on damage assessments and status of restoration efforts within the affected area is generally through the ESF structure, using established reporting protocols at the JFO and the NOC/NRCC. These field-level reports are the basis for CI/KR-related damage assessments and response and recovery activities.

CI/KR Incident-Related Assessments. When an incident occurs, assessments of sector-specific and cross-sector impacts are coordinated by DHS/OIP in collaboration with SSAs, GCCs, SCCs, ESFs, other appropriate agencies, and security partners. The assessments are supported by the integration of multiple data sets, to inform decisionmakers at all levels as they develop action recommendations.

DHS/OIP uses the NIPP risk management framework to analyze the implications that CI/KR affected by the incident may have on a regional or national basis. These include assessments to determine:

- Risk (consequence, vulnerability, and threat).
- Interdependencies.
- Cascading effects.
- Impact analyses inside and outside the affected area.

At the national level, the NISAC may conduct updates to existing assessments or perform new assessments to provide the most current situation data to decisionmakers.

NISAC products are made available to the NOC Planning Element, the Unified Coordination Group through the Infrastructure Liaison, and, as appropriate, other incident management and security partners involved in response activities.

Information included in the NADB is used to facilitate CI/KR identification within the impacted area and across the Nation that may be directly or indirectly affected by the cascading effects of the incident.

Regional-level assessments during response activities help inform leadership as to the best possible prioritization for CI/KR recovery and restoration.

Damage assessments are conducted by various teams that survey and assess impacts to CI/KR. The teams include, but are not limited to the following:

- Joint preliminary damage assessment teams estimate the extent of damages that could qualify for Federal assistance under the Stafford Act.
- Engineering teams assess impacts to specific elements of the infrastructure.
- Building process engineering teams.
- Environmental impact assessment teams.

The Infrastructure Liaison may provide CI/KR expertise and analyses to these teams as required.

The Infrastructure Liaison, in consultation with SSAs, ESF representatives, and others, as well as DHS/OIP representatives positioned within the various NOC components, develops and provides priorities recommendations regarding CI/KR to the Unified Coordination Group. These recommendations are based on ongoing access to national-level risk assessment and evaluation tools used to provide sector-by-sector and cross-sector evaluations of risk to and effects on CI/KR within and outside the incident area. These assessments are used to analyze CI/KR protection and restoration needs, support the efficient prioritization of efforts to meet these needs, and monitor the execution of support to CI/KR owners and operators.

Requests for assistance from CI/KR entities for incident-related requirements can be addressed through direct actions by owners and operators or with government assistance provided by Federal, State, tribal, or local authorities in certain specific circumstances. These requests must be directed to the appropriate Federal, State, tribal, and/or local decisionmakers with authority to consider and adjudicate requirements in the context of competing priorities.

At the State, tribal, or local level, requests for assistance from CI/KR owners and operators typically will be acted upon by State or local primacy or regulator agencies and/or within multiagency coordination centers in the affected area, such as the State or local EOC. CI/KR owners and operators of public or quasi-public infrastructure in the affected area are required to follow the established application process for Stafford Act disaster assistance.

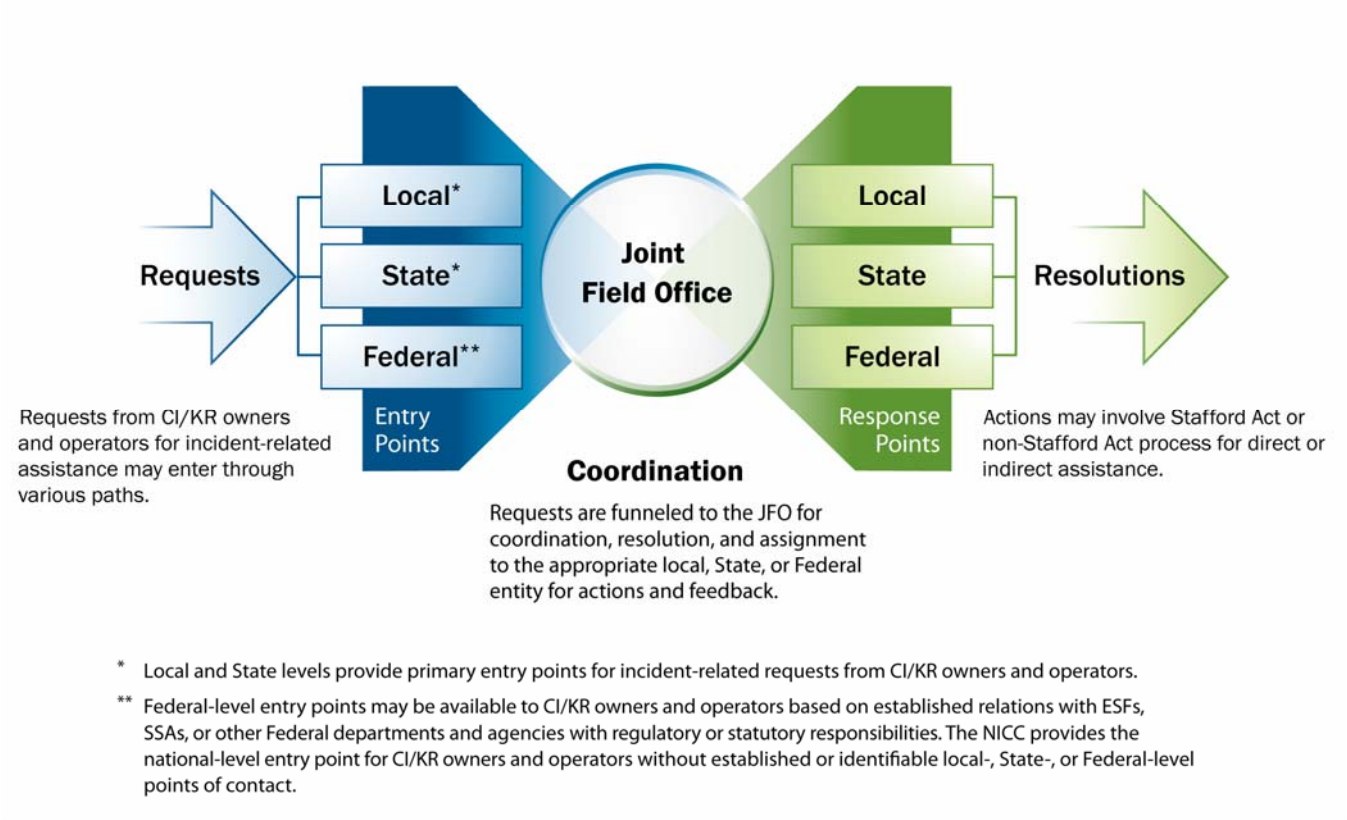
At the Federal level, requests may be addressed through existing authorities of Federal departments or agencies or through application of the Stafford Act. The JFO, when activated, is the Federal focal point at the field level for considering, adjudicating, and acting upon requests for assistance. In cases where a JFO has not been established, the NRCC provides the national-level forum for decisions and actions relating to the Federal assistance or resource support.

The Federal Coordinating Officer or Federal Resource Coordinator at the JFO (or the Operations Section Chief at the NRCC before establishment of a JFO) determines whether a request submitted by the State on behalf of a CI/KR owner or operator or by a Federal department or agency through ESF #5 – Emergency Management is valid and supportable.

When the request involves application of Stafford Act authorities, the determination is based on consideration of a number of factors that include, but are not limited to, the following questions:

- Is assistance essential to public health and safety?
- Is a specific authority, such as the Stafford Act or DPA, needed for the request?
- Does the JFO have the capability to provide resources through Stafford Act authorities or to facilitate non-Stafford Act coordination to meet the requirement?
- Does the request align with current response, recovery, and restoration priorities established by the Unified Coordination Group or through the NRCC if the JFO is not established?
- Is the Federal Government the most appropriate level to provide resources to meet the requirement? If so, what ESF is the most appropriate to coordinate the request?
- What is the reimbursement mechanism for ESF or other Federal department or agency support?
- Which other officials are participating in the Unified Coordination Group or at the national level and are able to commit agency authorities or resources that would be needed to support the request?
- Does the request align with the current incident-management priorities?
- Does the requester have the capability to provide resources on its own?
- Are there alternative means and timing available to provide the requested assistance?
- What is the benefit or cost of providing assistance to a local community's resources, capabilities, and/or economy; meeting critical regional or national CI/KR needs; and/or redirecting the requested resource or capability from other requirements?

Figure 2. Requests for Assistance From CI/KR Owners and Operators



CI/KR-related requests for incident-related assistance may come in through various paths at the local, State, regional, or national level. (See Figure 2.) Requests for assistance or information from CI/KR owners and operators may relate to a variety of incident-related needs such as requirements for security, impact area access, fuel, or accommodations for crews needed to perform critical repair work.

Regardless of the entry point, requests are coordinated, tracked, and channeled to the appropriate authorities and CI/KR subject-matter experts from the appropriate cooperating agencies for resolution and determination of the best course of action.

Generally, State, tribal, and local authorities and/or SSAs, ESF primary or supporting agencies, or other Federal Government entities, including those with regulatory responsibilities, provide primary entry points for these requests.

Entry points and processing paths, depicted in Figure 2 above, are as follows:

- Local and State officials, in most cases, determine the appropriate level at which to consider and/or coordinate support to ensure the most effective response to requests for assistance from private-sector CI/KR owners and operators. Local authorities may elect to fill valid requests using local resources. If local resources are not available, they may utilize mutual aid and assistance agreements to access additional resources.

- If all local resources are depleted, including those that can be acquired through mutual aid and assistance agreements, then local officials may forward the request to the State for action. The State may also elect to fill valid requests using its assets or request support from another State using the Emergency Management Assistance Compact or other preestablished memorandums of understanding. If assistance is not available at the State level, officials may forward the request to the JFO (or NRCC if the JFO is not established) to determine whether the request is eligible for Federal assistance.

- In CI/KR sectors where there is no primary State or local point of contact, representatives of the various ESF, SSA, and/or Federal regulatory authorities positioned within the NRCC, Regional Response Coordination Centers, and/or the JFO serve as points of contact. In these sectors, owners and operators communicate requests through the established relationship with the Federal department or agency that has primary responsibility for a specific functional area. The SSA and/or ESF may address a CI/KR-related request it deems to be valid using its own authorities or resources, if applicable, or may forward the request to the NRCC or the JFO through ESF #5 for further consideration.

The NICC provides an alternate avenue for CI/KR owners and operators to communicate needs for assistance, and is the most appropriate path in situations in which CI/KR owners and operators do not have either mechanisms for coordination at the local or State levels or established linkages to ESFs, SSAs, or other Federal entities that can help communicate and facilitate the requests. The NICC is the appropriate point of entry in the following circumstances:

- Before JFO establishment.

- National-level, nongeographic-specific incidents that do not require JFO establishment (such as response to terrorist threat or biological, agricultural, or other widespread incident).

- Specific CI/KR asset, system, network, or function of national significance based on scope or potential impact or criticality to national security or economic vitality.

Requests submitted to the NICC are routed, as appropriate, through the NRCC or the Unified Coordination Group, and the Infrastructure Liaison for coordination with the appropriate ESF, SSA, and other coordinating and cooperating agencies.

The NICC maintains an automated log of all requests for assistance or information it has processed. This log is shared with the Infrastructure Liaison at the JFO and DHS/OIP to maintain ongoing situational awareness, avoid duplication of effort, and enable coordination of actions relevant to the request.

Prior to full activation of the JFO, the NICC works closely with the NRCC to coordinate requests for assistance from CI/KR owners and operators.

Activation and Deployment. DHS/OIP, in coordination with the NRCC and the JFO, designates and deploys staff to support Infrastructure Liaison activities at the national and field levels. These deployed field elements maintain close coordination with national elements at the NOC, NRCC, and NICC.

The Infrastructure Liaison(s) support prevention, preparedness, response, and recovery in the following manner:

- Facilitating CI/KR situational awareness, assessment, and information sharing by providing liaison with the DOJ/FBI SIOC and other Federal emergency operations centers, initial operating facilities, or other incident management facilities established consistent with the specific threat or incident.
- Facilitating the CI/KR information-sharing process through coordination with JFO sections, ESF and sector representatives, CI/KR owners and operators, and other security partners at the field level.
- Providing information on CI/KR risk, damage, and service disruption within the impact area. This information is coordinated with national elements outside the affected area including identification of CI/KR that may pose a higher level of concern as a result of the incident.
- Facilitating development of courses of action relating to CI/KR restoration to provide continuity of essential goods and services.
- Providing a point of contact for CI/KR sectors that do not have direct alignment with a specific ESF (such as postal and shipping, commercial facilities, and national monuments and icons).
- Participating, as requested, in preliminary damage assessments, rapid needs assessment, Federal Incident Response Support Teams, and others.
- Coordinating with ongoing damage and security assessments to eliminate duplication of effort and promote sharing of assessment results.
- Providing situational awareness in regard to CI/KR assets and cross-sector concerns to the JFO, in coordination with the NRCC and DHS/OIP.
- Participating in JFO senior leadership and activities required for the operational planning cycle and development of the Incident Action Plan.
- Monitoring execution of support to CI/KR entities as required by the Incident Action Plan.
- Ensuring sensitive CI/KR related information is handled and safeguarded in accordance with the Protected Critical Infrastructure Information (PCII)[15] program or other appropriate guidelines.
- Assessing CI/KR protection and restoration needs to support efficient prioritization of efforts to meet requirements.

[15] The PCII Program, which operates under the authority of the Critical Infrastructure Information (CII) Act of 2002, provides a means for sharing private-sector information with the government while providing assurances that the information will be exempt from public disclosure and will be properly safeguarded. This program defines the requirements for submitting critical infrastructure information as well as the requirements that government entities must meet for accessing and safeguarding PCII.

- Directing activities of DHS/OIP field staff in geographic branches (as designated by the JFO) based on priorities established by the Infrastructure Liaison.

- Resolving information discrepancies relating to status of CI/KR restoration and protection activities in various sections of the JFO.

- Participating in JFO "hotwashes" to identify CI/KR-related issues.[16]

- Maintaining automated linkage to the NICC.

- Tracking and coordinating with ESFs and SSAs on private-sector requests for assistance and requests for information when required to provide cross-sector facilitation.

- Coordinating with ESFs, SSAs, and appropriate Federal agencies to identify and aggregate CI/KR-related concerns and security requirements.

The Infrastructure Liaison develops CI/KR protection and restoration priority recommendations in coordination with JFO section and branch managers and representatives of ESF primary and supporting agencies. Infrastructure Liaison coordination activities with ESF representatives include:

- Developing coordinated inputs for the Incident Action Plan.

- Coordinating with activated ESFs on recovery, restoration, and security requirements, specifically to include coordinating with:

  - ESF #1 for transportation infrastructure.
  - ESF #2 on the status of communications infrastructure operations.
  - ESF #3 on infrastructure risk and vulnerability assessments.
  - ESF #8 on status and impacts on the public health and medical community.
  - ESF #11 on agricultural, natural and cultural resources, and historic properties issues.
  - ESF #12 on impact assessments for the energy infrastructure.
  - ESF #13 on efforts to analyze protection requirements and/or enhance security and protection measures for CI/KR within and outside the affected area.
  - ESF #14 on long-term community recovery, including impacts on commercial and banking and finance entities.

(Further discussion of specific ESF responsibilities is included in the respective ESF Annexes to the NRF.)

Incident-Related Communication, Including Emergency Public Information. The DHS Office of Public Affairs (DHS/PA), at the national level, works in conjunction with DHS/OIP and the DHS Assistant Secretary for the Private Sector to provide timely public information to the CI/KR sectors and their security partners (through conference call, e-mail, or both) during national-level incidents that require a coordinated Federal response.

The CI/KR incident communications system is modeled after processes outlined in the NRF Public Affairs Support Annex to ensure coordination with Federal, State, tribal, and local entities.

[16] Interagency meetings called "hotwashes" are convened to identify critical issues, lessons learned, and best practices associated with incident management activities. Hotwashes typically are conducted at major transition points over the course of incident-related operations, and include Federal, State, tribal, local, and other participation as appropriate.

DHS/PA communication actions include the following:

- Providing the overarching coordination lead for incident communications to the public during an incident requiring a coordinated Federal response.
- Maintaining a standing conference line for use by CI/KR incident communications coordinators.
- Coordinating and disseminating line access information in coordination with DHS/OIP.
- Maintaining a contact list, including e-mail information, of CI/KR incident communications coordinators.
- Coordinating with SSAs to share public information and messages for SCCs and GCCs.

DHS/PA works in coordination with ESFs and SSAs to identify organizations and/or individuals (e.g., SCCs, major trade associations, State and local regulatory entities) to act as focal points for incident communications with the private sector. These organizations and individuals are selected based on their ability to disseminate information to and coordinate with a broad array of other organizations and individuals.

Representatives serve as the primary reception and transmission points for incident communications products from DHS/PA, ESFs, and SSAs, and they retain responsibility for dissemination to counterpart communicators to ensure information is distributed widely.

POSTRESPONSE ACTIONS

As an incident is brought to closure, incident-related activities transition back from response to steady state. Concurrently, the after-action report is prepared.

Demobilization. CI/KR-related liaison, coordination, and information-sharing activities continue in support of JFO functions as required and continue at a level consistent with ongoing efforts.

Infrastructure Liaison actions include the following:

- Participating in JFO "hotwashes" to identify critical CI/KR-related issues.
- Evaluating CI/KR support staffing requirements and making recommendations for redeployment of staff members to the Unified Coordination Group.
- Preparing plans for deactivation and transfer of responsibilities to DHS/OIP, the NICC, or other elements, as appropriate.
- Coordinating with the JFO Planning Section on CI/KR-related long-term recovery efforts.
- Providing input to the local or regional demobilization strategy.
- Informing onsite leadership or a designated representative of the overall DHS/OIP demobilization strategy.

Non-DHS/OIP deployed response elements execute their respective organizational demobilization plans.

The NICC maintains the reporting and information-sharing tempo in coordination with the NOC, NRCC, and JFO requirements. As requirements diminish, the NICC notifies cooperating agencies of reporting requirement changes and other incident-related activities throughout the incident closure process.

After-action reports are developed following an incident to detail operational successes, problems, and key issues affecting management of the incident. After-action reports include appropriate feedback from all Federal, State, tribal, local, nongovernmental, and private-sector partners participating in the incident.

Procedures to complete after-action reports include:

- DHS/OIP organizing and managing a template to capture CI/KR data.
- CI/KR security partners collecting/collating and submitting relevant after-action data[17] throughout the incident life cycle.
- CI/KR security partners participating in after-action evaluation sessions at the national and the regional levels.

DHS/OIP coordinates review meetings after the conclusion of the incident and publication of after-action reports to ensure that lessons learned concerning CI/KR issues throughout the incident are accurately captured and integrated into plans, assessments, and procedures across all agencies.

The NICC ensures that after-action information is posted to the network and is available to security partners as appropriate.

RESPONSIBILITIES

Coordinating Agency: DHS

DHS, as the department charged with overarching responsibility for coordination of CI/KR identification, protection, and prioritization, is the coordinating agency for the CI/KR Support Annex. In this context, DHS, in collaboration with SSAs, is responsible for the following:

- Developing plans, processes, guidance, and partnerships and facilitating coordinated CI/KR protection with the private sector at the strategic, operational, and tactical levels both during steady-state, day-to-day operations and during incident response.
- Sharing and protecting information on sensitive CI/KR-related matters such as threats, warnings, response activities, and operational status—before, during, and after an incident.
- Identifying, training, designating, and deploying personnel to support the Infrastructure Liaison role and staff members in the JFO and its area of operations.
- Informing and educating private-sector owners and operators; State, tribal, and local governments; and other security partners on NRF and NIPP content, and encouraging and facilitating the development and coordination of equivalent planning for CI/KR protection both for steady-state operations and during an incident.

[17] Data relevant for after-action reports can originate from written reports, meeting notes, interviews, briefings, observations, communications, and other recordings.

- Coordinating and conducting national and regional incident management exercises, training events, and working meetings with the private sector and State, local, tribal, and select foreign governments.

- Developing methodology to track requests for information from or assistance to CI/KR facilities to help ensure that responding departments and agencies are aware of requests from or visits made to CI/KR facilities.

- Developing, implementing, and operating information-sharing and communication strategies, processes, and systems with CI/KR security partners.

Cooperating Departments and Agencies

This section discusses responsibilities of all cooperating agencies, including those that are specific to SSAs, ESFs, other departments and agencies, and CI/KR owners and operators. In addition to the cooperating agencies designated in this section, departments and agencies with primary responsibility for each of the ESFs are responsible for developing and maintaining working relations with associated private-sector counterparts and for exercising ESF mechanisms to enable the recovery of CI/KR. Cooperating agencies for this annex may concurrently have responsibilities as ESF primary or supporting agencies, or as coordinating or cooperating agencies for other NRF Support or Incident Annexes.

In accordance with the NRF, all cooperating agencies are responsible for the following:

- Working in collaboration with CI/KR private-sector security partners, owners, and operators.

- Conducting operations relating to CI/KR identification, prioritization, and protection using their own authorities, subject-matter experts, capabilities, or resources.

- Participating in planning for short-term and long-term CI/KR-related incident management, response, recovery, and restoration functions and for the development of supporting operational plans, standard operating procedures, checklists, or other job aids.

- Providing available personnel, equipment, or other resource support.

- Participating in training and exercises aimed at continuous improvement of CI/KR-related prevention, response, and recovery capabilities.

- Using established Incident Command System, EOC, NOC, and/or JFO information-sharing protocols to notify 1) other agencies that may have overlapping responsibilities for a CI/KR asset, system, or network of intended actions concerning requests for information from or assistance to a CI/KR facility or 2) of field visits to such facilities.

- Nominating to DHS for review and evaluation new technologies or procedures that have the potential to improve performance within or across CI/KR protection functional areas.

Sector-Specific Agencies

In the context of this annex, SSAs are responsible for the following incident-related actions:

- Identifying, prioritizing, and coordinating Federal action in support of the protection of nationally critical assets, systems, and networks, with a particular focus on CI/KR that could be exploited to cause catastrophic health effects or mass casualties.
- Collaborating with State and private-sector security partners to facilitate real-time incident notification, as well as CI/KR protection expertise and risk assessment methods in the sector.
- Establishing coordination mechanisms for CI/KR protection during response and recovery.
- Participating in planning and implementation of recovery measures, as required, in coordination with processes established in the NRF for related ESF Annexes and other Incident and Support Annexes.
- Providing comprehensive risk assessment and management programs, as appropriate and consistent with the unique sector landscape, that can be used for identifying protection priorities for incident-related situations.
- Working with all security partners to develop plans and processes for threat-based increases in protective measures that align the CI/KR protective posture to all-hazards warnings, specific threat indications, and the different levels of the HSAS.

Emergency Support Functions

In the context of this annex, ESF primary and supporting departments and agencies are responsible for developing and maintaining working relationships with associated State, local, and private-sector counterparts and exercising their ESF mechanisms to enable the recovery of CI/KR. This includes, but is not limited to, the following:

- Establishing and implementing processes to ensure full integration of CI/KR-related activities relevant to the specific ESF and including these processes in the respective ESF Annex to the NRF.
- Coordinating with CI/KR owners and operators, as appropriate.
- Coordinating with the DHS/OIP representative at the NOC and with the JFO Infrastructure Liaison.
- Providing CI/KR-related damage assessments and operating status in the affected area using established JFO and NOC reporting procedures.
- Responding to or coordinating CI/KR-related requests for assistance as relevant to the specific ESF.

COOPERATING AGENCIES

Agency	Functions
Department of Agriculture (USDA)	• Serves as the SSA for the Agriculture and Food Sector. • Advises and assists in assessing impacts to meat, poultry, and egg products.
Department of Commerce	• Works with DHS and private-sector, research, academic, and government organizations to improve cyber system technology and promote other CI/KR protection efforts, including use of authority under the DPA to ensure timely availability of industrial products, materials, and services to meet homeland security requirements and address economic security issues. • Supports the Emergency Alert System through the National Oceanic and Atmospheric Administration (NOAA)/National Weather Service and provides public dissemination of critical preevent and postevent information over the all-hazards NOAA Weather Radio system, the NOAA Weather Wire Service, and the Emergency Managers' Weather Information Network.
Department of Defense	Serves as SSA for the Defense Industrial Base Sector, when requested, and, upon approval of the Secretary of Defense, provides Defense Support of Civil Authorities (DSCA) during domestic incidents. Accordingly, the Department of Defense is considered a cooperating agency under this annex.
Department of Education	• Provides guidance and information to the education community regarding education facility protection, both public and private, as a subsector of Government Facilities Sector. • Works with the Government Facilities Sector to help ensure the Education Subsector gets appropriate attention in steady-state protection efforts as well as in the incident management environment.
Department of Energy	• Maintains the United States' continuous and reliable energy supplies through preventive measures as well as supporting restorative actions. • Serves as SSA for the Energy Sector.
Department of Health and Human Services (HHS)	• Serves as the designated SSA for the Healthcare and Public Health Sector. • Through the Food and Drug Administration, serves as the SSA for food other than meat, poultry, and egg products portion of the Food and Agriculture Sector. • Is the primary agency for ESF #8 – Public Health and Medical Services coordinating resources for public health and medical and serves as a support agency to ESF #6 – Mass Care, Emergency Assistance, Housing, and Human Services.
Department of the Interior (DOI)	• Advises and assists in assessing impacts to natural resources, habitats, wildlife, subsistence uses, public lands, Indian tribal lands, and cultural areas. • Serves as the SSA for the National Monuments and Icons Sector.
Department of Justice	Reduces terrorist threats and investigates and prosecutes actual or attempted attacks on, sabotage of, or disruptions to CI/KR in collaboration with DHS.
Department of Labor	Through the Occupational Safety and Health Administration, provides worker safety advice, assistance, and policy support for CI/KR-related activities.
Department of State	Works with foreign governments and international organizations to strengthen U.S. CI/KR protection efforts.
Department of Transportation (DOT)	• Collaborates with DHS on matters of transportation security and transportation infrastructure protection, and is additionally responsible for operating the National Airspace System. • Collaborates with DHS to regulate transportation of hazardous materials (all modes), including pipelines.

Agency	Function
Department of the Treasury	• Assesses incident impact to the Banking and Finance Sector. • Provides expertise on the overall economic impact to CI/KR. • Serves as the Primary Economic Advisor to the President. • Serves as the SSA for the Banking and Finance Sector and collaborates with other vital CI/KR sectors to foster information sharing regarding cross-sector vulnerabilities and protective measures within the sector.
Department of Veterans Affairs	• Contributes extensive expertise to both the Government Facilities and Public Health and Healthcare Sectors through active participation in its respective GCC. • Serves as a supporting agency for a number of ESFs, providing coordination with the medical system as well as direct resources and support for incident management efforts.
Environmental Protection Agency	• Serves as the SSA for the Drinking Water and Water Treatment Systems Sector. • Serves as primary agency for the ESF #10 – Oil and Hazardous Materials Response Annex, support agency for the ESF #3 – Public Works and Engineering Annex, and coordinating agency for the Nuclear/Radiological Incident Annex. • Performs oil and hazardous materials as well as water and wastewater response and recovery activities.
Federal Energy Regulatory Commission	• Regulates interstate transmission of electricity, natural gas, and oil. • As an independent agency, reviews proposals to build liquefied natural gas terminals and interstate natural gas pipelines and licenses hydropower projects. • Through the Office of Dam Safety, regulates approximately 2,100 dams that generate electricity.
The Intelligence Community	• Provides vital service to identify and assess threats that may impact the Nation's CI/KR. • With the DOD and other appropriate Federal departments, such as DOI and DOT, collaborates with DHS on development and implementation of geospatial programs to map, image, analyze, and sort CI/KR data. • Serves as a source of intelligence information necessary for CI/KR protection. DHS works with Federal departments and agencies to identify and help protect those positioning, navigation, and timing services that are critical enablers for CI/KR sectors. • Collaborates with DHS and other agencies, such as the Environmental Protection Agency, that manage data addressed by Geographic Information Systems.
Nuclear Regulatory Commission (NRC)	• Ensures the protection of the health and safety of the public or the common defense and security involving the use of NRC-licensed radioactive materials in commercial nuclear reactors for electric power generation and non-power nuclear reactors for research, testing, and training; medical, industrial, and academic uses of radioactive materials, and facilities that fabricate nuclear fuel; and transportation, storage, and disposal of nuclear materials and waste. • Closely coordinates its actions with its licensees, DHS, other Federal agencies, and State and local government officials during radiological incidents by providing advice, guidance, and support as needed. • Performs independent assessments of incidents and potential offsite consequences and, as appropriate, provides recommendations concerning any protective measures.
Office of Science and Technology Policy	Coordinates with DHS to further interagency research and development related to CI/KR protection.
U.S. Postal Service	Collects and reports on damage and disruption to the Postal and Shipping Sector as information becomes available.

Agency	Function
Information Sharing and Analysis Center (ISAC) Council	• Supports sector-specific information and/or intelligence requirements for incidents, threats, and vulnerabilities. • Provides secure capabilities for members to exchange and share information on cyber, physical, or other threats. • Establishes and maintains operational-level dialogue with appropriate governmental agencies, identifying and disseminating knowledge and effective practices.
Partnership for Critical Infrastructure Security (PCIS)	Coordinates cross-sector initiatives to support CI/KR protection. The PCIS membership is comprised of one or more members and their alternates from each of the CI/KR SCCs.

APPENDIX A: SECTOR-SPECIFIC AGENCIES FOR CRITICAL INFRASTRUCTURE AND KEY RESOURCES

The following list includes those Federal departments and agencies identified in HSPD-7 as responsible for CI/KR protection activities in specified CI/KR sectors.

Table A-1. Sector-Specific Agencies for Critical Infrastructure and Key Resources

Sector-Specific Agency	Critical Infrastructure/Key Resources Sector
Department of Agriculture[18]	Agriculture and Food
Department of Health and Human Services[19]	
Department of Defense[20]	Defense Industrial Base
Department of Energy[21]	Energy
Department of Health and Human Services	Public Health and Healthcare
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Drinking Water and Water Treatment Systems[22]
Department of Homeland Security	
Office of Infrastructure Protection	Chemical
	Commercial Facilities
	Dams
	Emergency Services
	Nuclear Reactors, Materials, and Waste
Office of Cyber Security and Communications	Information Technology
	Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration/U.S. Coast Guard[23]	Transportation Systems[24]
Immigration and Customs Enforcement/Federal Protective Service	Government Facilities

[18] USDA is responsible for agriculture and food (meat, poultry, and egg products).
[19] HHS is responsible for food other than meat, poultry, and egg products.
[20] Nothing in this plan impairs or otherwise affects the authority of the Secretary of Defense, including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures.
[21] The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.
[22] Drinking Water and Water Treatment includes drinking water supply, treatment, and distribution; and wastewater collection, treatment, and disposal.
[23] DHS/U.S. Coast Guard is the SSA for the maritime transportation mode.
[24] As stated in HSPD-7, DOT and DHS will collaborate on all matters relating to transportation security and transportation infrastructure protection.

APPENDIX B: RELATIONSHIP OF EMERGENCY SUPPORT FUNCTIONS TO CI/KR SECTORS

This table shows how the 15 Emergency Support Functions map to the 17 CI/KR sectors.

Table B-1. Relationship of Emergency Support Functions to CI/KR sectors

Emergency Support Function	Related CI/KR Sectors
ESF Primary Agencies: Coordinate Resources Support and Program Implementation for Response, Recovery, Restoration, and Mitigation programs directly related to incident management functions.	**Sector-Specific Agencies (SSAs)** Coordinate efforts to protect the Nation's CI/KR from terrorist attacks and for helping to strengthen preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.
ESF #1 – Transportation **Primary Agencies:** Department of Transportation DHS/Federal Emergency Management Agency	• **Transportation Systems** **SSA:** DHS/Transportation Security Administration • **Postal and Shipping** **SSA:** DHS/Transportation Security Administration • **Emergency Services** **SSA:** DHS/Infrastructure Protection
ESF #2 – Communications **Primary Agencies:** DHS/Cyber Security and Communications/National Communications System DHS/Federal Emergency Management Agency	• **Information Technology** **SSA:** DHS/Cyber Security and Communications • **Communications** **SSA:** DHS/Cyber Security and Communications/ National Communications System • **Emergency Services** **SSA:** DHS/Infrastructure Protection
ESF #3 – Public Works and Engineering **Primary Agencies:** DHS/Federal Emergency Management Agency DOD/U.S. Army Corps of Engineers	• **Drinking Water and Water Treatment Systems** **SSA:** Environmental Protection Agency • **Dams** **SSA:** DHS/Infrastructure Protection • **Energy** **SSA:** Department of Energy • **Emergency Services** **SSA:** DHS/Infrastructure Protection • **Government Facilities** **SSA:** DHS/Immigration and Customs Enforcement/ Federal Protective Service • **National Monuments and Icons** **SSA:** Department of the Interior
ESF #4 – Firefighting **Primary Agency:** USDA/Forest Service	• **Emergency Services** **SSA:** DHS/Infrastructure Protection • **Government Facilities** **SSA:** DHS/Immigration and Customs Enforcement/ Federal Protective Service
ESF #5 – Emergency Management **Primary Agency:** DHS/Federal Emergency Management Agency	• **Emergency Services** **SSA:** DHS/Infrastructure Protection • **Government Facilities** **SSA:** DHS/Immigration and Customs Enforcement/ Federal Protective Service

Emergency Support Function	Related CI/KR Sectors
ESF #6 – Mass Care, Emergency Assistance, Housing, and Human Services **Primary Agency:** DHS/Federal Emergency Management Agency	• **Emergency Services** **SSA:** DHS/Infrastructure Protection • **Public Health and Healthcare** **SSA:** Department of Health and Human Services
ESF #7 – Resource Support **Primary Agency:** General Services Administration	All
ESF #8 – Public Health and Medical Services **Primary Agency:** Department of Health and Human Services	• **Emergency Services** **SSA:** DHS/Infrastructure Protection • **Public Health and Healthcare** **SSA:** Department of Health and Human Services
ESF #9 – Search and Rescue **Primary Agencies:** DHS/Federal Emergency Management Agency DHS/U.S. Coast Guard	• **Emergency Services** **SSA:** DHS/Infrastructure Protection
ESF #10 – Oil and Hazardous Materials Response **Primary Agencies:** Environmental Protection Agency DHS/U.S. Coast Guard	• **Chemical** **SSA:** DHS/Infrastructure Protection • **Nuclear Reactors, Materials, and Waste** **SSA:** DHS/Infrastructure Protection • **Emergency Services** **SSA:** DHS/Infrastructure Protection
ESF #11 – Agriculture and Natural Resources **Primary Agencies:** Department of Agriculture Department of the Interior	• **Agriculture and Food** **SSA:** Department of Agriculture and Department of Health and Human Services/Food and Drug Administration • **National Monuments and Icons** **SSA:** Department of the Interior
ESF #12 – Energy **Primary Agency:** Department of Energy	• **Energy** **SSA:** Department of Energy • **Nuclear Reactors, Materials, and Waste** **SSA:** DHS/Infrastructure Protection
ESF #13 – Public Safety and Security **Primary Agency:** Department of Justice	• **Emergency Services** **SSA:** DHS/Infrastructure Protection • **Postal and Shipping** SSA: DHS/Transportation Security Administration • **All others as appropriate**
ESF #14 – Long-Term Community Recovery **Primary Agencies:** Department of Agriculture DHS/Federal Emergency Management Agency Department of Housing and Urban Development Small Business Administration	• **Banking and Finance** **SSA:** Department of the Treasury • **Commercial Facilities** **SSA:** DHS/Infrastructure Protection • **Drinking Water and Water Treatment Systems** **SSA:** Environmental Protection Agency

Emergency Support Function	Related CI/KR Sectors
ESF #15 – External Affairs **Primary Agency:** DHS/Federal Emergency Management Agency	All

Notes:

- When requested, and upon approval of the Secretary of Defense, DOD provides DSCA during domestic incidents. In the context of the NRF, DOD is considered a support agency for all ESFs. DOD is the SSA for the Defense Industrial Base sector, which may have links to many of the ESFs.

- As stated in HSPD-7, DOT and DHS will collaborate on all matters relating to transportation security and transportation infrastructure protection.

List of Acronyms

CFR	Code of Federal Regulations
CI/KR	Critical Infrastructure and Key Resources
CII	Critical Infrastructure Information
COP	Common Operating Picture
DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department of Justice
DOT	Department of Transportation
DPA	Defense Production Act
DSCA	Defense Support of Civil Authorities
EOC	Emergency Operations Center
ESF	Emergency Support Function
FBI	Federal Bureau of Investigation
GCC	Government Coordinating Council
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HSAS	Homeland Security Advisory System
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
JFO	Joint Field Office
NADB	National Asset Database
NCC	National Coordinating Center for Telecommunications
NCS	National Communications System
NICC	National Infrastructure Coordinating Center
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NISAC	National Infrastructure Simulation and Analysis Center
NOAA	National Oceanic and Atmospheric Administration
NOC	National Operations Center
NRC	Nuclear Regulatory Commission
NRCC	National Response Coordination Center
NRF	National Response Framework
NS/EP	National Security and Emergency Preparedness
OI&A	Office of Intelligence and Analysis
OIP	Office of Infrastructure Protection
PA	Office of Public Affairs
PCII	Protected Critical Infrastructure Information
PCIS	Partnership for Critical Infrastructure Security
PFO	Principal Federal Official
PSA	Protective Security Advisor
SCC	Sector Coordinating Council
SIOC	Strategic Information and Operations Center
SSA	Sector-Specific Agency
SSP	Sector-Specific Plan
US-CERT	United States Computer Emergency Readiness Team